REMARKS

This communication is a full and timely response to the non-final Office Action dated September 11, 2003. By this communication, Applicants have canceled claims 3, 6-8, and 12-16. Further claim 1 has been amended to incorporate the elements of claim 3, claim 9 has been amended to incorporate the elements of claim 12, and each of claims 1 and 9 have been amended to recite wherein the user's instruction is one of a decryption of encrypted text or an encryption of plain text, and the user's instruction is connected to the host computer via communication cable. Support for the changes to claims 1 and 9 can be found variously throughout the specification. For example, support for the amendment to claims 1 and 9 can be found in original claims 3 and 12, and in the specification at page 16 line 22 through page 17 line 24. Still further, claims 5 and 11 have been amended to recite, among other things, wherein the encrypted text is received from the host computer and the decrypted plain text is sent to the host computer. Support for the changes to claims 5 and 11 can be found variously throughout the specification. For example, support for the changes to claims 5 and 11 can be found in the specification at 16 line 22 through page 17 line 24. In addition, claims 2, 4, and 10 have been amended to improve form. No new matter has been added. Claims 1, 2, 4, 5, 9, 10, and 11 are pending where claims 1 and 9 are independent.

Rejections Under 35 U.S.C. §102

Claims 1-14 were rejected under 35 U.S.C. §102(a) as anticipated by *Pare Jr. et al.*, U.S. Patent No. 5,838,812. By this amendment, claims 3, 6-8, and 12-14 have been canceled, thereby rendering this portion of the rejection moot. Applicants respectfully traverse this rejection.

Independent claim 1 recites an authentication system used when stored information is manipulated, comprising, a host computer comprising input means for inputting a user's instruction; command output means for generating from the user's instruction an instruction command which requests a predetermined processing to be executed and for outputting the instruction command; and communication means for communicating with an external unit; and a fingerprint identification apparatus comprising, communication means for communicating with said host computer; processing control means for executing a predetermined processing according to the instruction command input from said host computer by said communication means; fingerprint detection means for detecting a fingerprint and for generating fingerprint data; storage-information recording means for recording the fingerprint data and storage

5

information related to the fingerprint data; and fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by said storage-information recording means, wherein said storage-information recording means stores a private key generated by the public-key encryption method, and wherein the user's instruction is one of a decryption of an encrypted text and an encryption of plain text, and the user's instruction is sent to the host computer through communication cable.

Independent claim 9 recites an authentication method used when stored information is manipulated, comprising the steps of a host computer informing a user of a fingerprint-identification request according to a user's instruction and issuing a fingerprint-identification instruction command to a fingerprint identification apparatus; the fingerprint identification apparatus reading a fingerprint after the user places a finger on the fingerprint identification apparatus, verifying the read fingerprint with a stored fingerprint, and sending a fingerprint-identification result to the host computer; the host computer allowing the user to specify the next instruction when the result is affirmative, and issuing the instruction command corresponding to the next instruction; and the fingerprint identification apparatus accessing storage information according to the instruction command and executing a predetermined processing, wherein said storage-information recording means stores a private key generated by the public-key encryption method, and wherein the user's instruction is one of a decryption of an encrypted text and an encryption of plain text, and the user's instruction is sent to the host computer through communication cable.

Pare Jr. discloses a system for identifying individuals for the purpose of performing financial transactions and non-financial transmissions, which can accommodate a large number of users. In particular, a data processing center 1 connects to various terminals 2 and computer networks 4 through a various types of communication mediums 3. A firewall machine 5 prevents electronic intrusion of the system and a gateway machine 6 executes the requests of the users, and decrypts data received from the various terminals. The various terminals can be any of a number of data entry and biometric devices 13. The terminal 2 communicates to other devices on the network via a conventional modem 18 using request packets 19 and response packets 20. During communication, certain portions of the request packets 19 and response packets 20 are encrypted while other portions of these packets are sealed. In particular, a when sending information to a data processing center 1, the biometric device 13 outputs an encrypted biometric–PIC block that includes a message key. That is each biometric-PIC block received by

the data processing center 1 may also contain an optional response key. Before responding to a request that includes a response key, the DPC encrypts the reply packet with the response key. *Pare, Jr.*, however, fails to disclose, teach, or suggest at least that the user's instruction is one of a decryption of encrypted text or an encryption of plain text, and the user's instruction is connected to the host computer via communication cable.

Claims 1 and 9 recite, among other things, wherein the user's instruction is one of a decryption of encrypted text or an encryption of plain text, and the user's instruction is connected to the host computer via communication cable. To properly anticipate a claim, the document must disclose, explicitly or implicitly, each and every feature recited in the claim. *See* Verdegall Bros. v. Union Oil Co. of Calif., 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). For at least the reasons discussed above, Applicants respectfully request that the rejection of claims 1 and 9 under 35 U.S.C. §102 be withdrawn, and these claims be allowed.
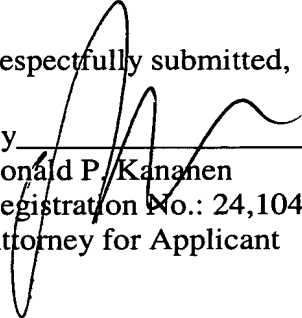
Claims 2, 4, and 5 depend from claim 1, and claims 10 and 11 depend from claim 9. By virtue of this dependency, Applicants submit that claims 2, 4, 5, 10, and 11 are allowable for at least the same reasons given above with respect to their respective base claims. In addition, Applicants submit that claims 2, 4, 5, 10, and 11 are further distinguished over *Pare, Jr.* by the additional elements recited therein, and particularly with respect to each claimed combination. Applicants respectfully request, therefore, that the rejection of claims 2, 4, 5, 10, and 11 under 35 U.S.C. §102 be withdrawn, and these claims be allowed.

Conclusion

Based on at least the foregoing amendments and remarks, Applicants submit that claims 1, 2, 4, 5, and 9-11 are allowable, and this application is in condition for allowance. Accordingly, Applicants request favorable reexamination and reconsideration of the application. In the event the Examiner has any comments or suggestions for placing the application in even better form, Applicants request that the Examiner contact the undersigned attorney at the number listed below.

Dated: November 4, 2003

Respectfully submitted,

By_____
Ronald P. Kananen
Registration No.: 24,104
Attorney for Applicant

RADER, FISHMAN & GRAUER, PLLC
Lion Building
1233 20th Street, N.W., Suite 501
Washington, D.C. 20036
Tel: (202) 955-3750
Fax: (202) 955-3751
Customer No. 23353

DC137464